AMENDMENTS TO THE SPECIFICATION:

1. Please amend paragraph [0036] as follows:

[0036] Referring to FIG. 1, an intrusion detection network 10 includes user systems 12, 14 and 16. Each of the user systems 12, 14 and 16 is connected to a network of computers such as the Internet 18. A server system 20 and 22 are linked to the Internet 18. An example server system is a web server such as an Apache web server ~~(see http://www.apache.org)~~ (see www.apache.org). In general, the servers 20 and 22 each execute a computer program that provides services to other computer programs in the same or other computers, such as user systems 12, 14 and 16. In a client/server programming model, each of the server systems 20 and 22 executes a program that awaits and fulfills requests from client programs in the same or other computers, such as the user systems 12, 14 and 16. Fulfillment of a request is generally referred to as a response.

2. Please amend paragraph [0098] as follows:

[0098] The common format may be an Emerald format as designed by SRI International, Inc. of Palo Alto, Calif., and incorporated by reference herein ~~(see http://www.sri.com)~~ (see www.sri.com).

3. Please amend paragraph [0137] as follows:

[0137] The funneling process 56 communicates with the analysis engine 58 that is typically located in an external host and not in the web server 20. The funneling process 56, in an Emerald framework, accepts incoming connections where Emerald messages can be transmitted, and passes the information to outgoing connections. The funneling process 56 can duplicate incoming information (having two different analysis engines for the same application) or multiplex several incoming flows into one outgoing connection (comparing the results of a network-based monitor with an application integrated module for discrepancies). The funneling process 56 takes into account problems that might appear in interprocess communication, such as lost connections or

necessary buffering. An example analysis engine 58 is the Emerald expert from SRI International, Inc., incorporated by reference herein ~~(see http://www.sri.com)~~ (see www.sri.com). The Emerald expert analysis engine is a highly targetable signature-analysis engine based on the expert system shell P-BEST (Production-Based Expert System Toolset). Under Emerald's expert architecture, event-stream-specific rule sets are encapsulated within resource objects that are then instantiated within an Emerald monitor. The objects can then be distributed to an appropriate observation point in the computing environment. This enables a spectrum of configurations from lightweight distributed expert signature engines to heavy-duty centralized host-layer expert engines, such as those constructed for use in expert's predecessors, NIDES (Next-Generation Intrusion Detection Expert System), and MIDAS (Multics Intrusion Detection Alerting System). In a given environment, P-BEST-based experts may be independently distributed to analyze the activity of multiple network services (e.g., FTP, SMTP, HTTP) or network elements (e.g., a router or firewall). As each Emerald expert is deployed to its target, it is instantiated with an appropriate resource object (e.g., an FTP resource object for FTP monitoring), while the expert code base remains independent of the analysis target.